BULL. AUSTRAL. MATH. SOC. 13F20
VOL. 41 (1990) [381–386]

NORMS IN POLYNOMIAL RINGS

G. MYERSON

We give a formula for the norm on a polynomial ring modulo an ideal in terms of the zero–set of the ideal. We hint at the relation to resultants.

1. DEFINITIONS AND STATEMENT OF THEOREM

Let A be a ring (by which we mean a commutative ring with unity). Let B be a ring containing A, and suppose that, as an A-module, B is finitely–generated and free. Let b be any element of B; then multiplication by b is an A-linear operator T_b on B. The *norm* from B to A of b, written $N_A^B b$, is defined to be the determinant of T_b.

Perhaps the most familiar example is that in which A is the rationals and B is a number field; $N_A^B b$ then coincides with the field norm of algebraic number theory.

In what follows, we write A_n for $A[x_1, \ldots, x_n]$.

THEOREM. *Let A be an integral domain, and let I be an ideal in A_n such that $B = A_n/I$ is, as an A-module, finitely–generated and free. Let k be an algebraically closed field containing A, and let $Z(I)$ be the set of all zeros of I over k. Then $Z(I)$ is finite and, if f is in A_n, then*

$$N_A^B \overline{f} = \prod_{P \in Z(I)} f(P)^{m_P} \tag{1}$$

where $\overline{f} = f + I$ is the image of f in B, and m_P is the multiplicity of P as a zero of I.

Multiplicity is used here in the standard sense of algebraic geometry — we elaborate on this in the course of the proof. We note that the condition on I is quite restrictive; for example, if A is the ring of integers and n is 1 then I must be principal with monic generator. Steve Schanuel has suggested that B need only be projective, not free, but we have not explored this idea.

Received 6 June 1989

https://doi.org/10.1017/S0004972700018244 Published online by Cambridge University Press

2. Proof of part of the theorem

We believe that the finiteness of $Z(I)$ (under the hypotheses of the theorem) is due to Gröbner [3]. For the reader's convenience, we present a simple proof.

Proof: (of the finiteness of $Z(I)$). For a given j, $1 \leqslant j \leqslant n$, we consider the elements $1, x_j, x_j^2, \ldots,$ of A_n. Their images $1, \overline{x}_j, \overline{x}_j^2, \ldots$ in B cannot be A-linearly independent, since B is finitely-generated as an A-module; thus there exists a positive integer r and elements $a_0, \ldots, a_r$ of A such that $a_0 + a_1\overline{x}_j + \ldots + a_r\overline{x}_j^r = 0$ in B. Let $f_j(\underline{x}) = a_0 + a_1x_j + \ldots + a_rx_j^r$; then $\overline{f}_j = 0$, so $f_j \in I$. Now let $P = (\alpha_1, \ldots, \alpha_n)$ be in $Z(I)$. Then $f_j(P) = 0$, so $a_0 + a_1\alpha_j + \ldots + a_r\alpha_j^r = 0$, so there are only finitely many possible values for α_j. But j was arbitrary, so there are only finitely many points in $Z(I)$. □

3. Change of base, and Nullstellensatz

We wish to reduce the theorem to the case where $A = k$, that is, where A is an algebraically closed field.

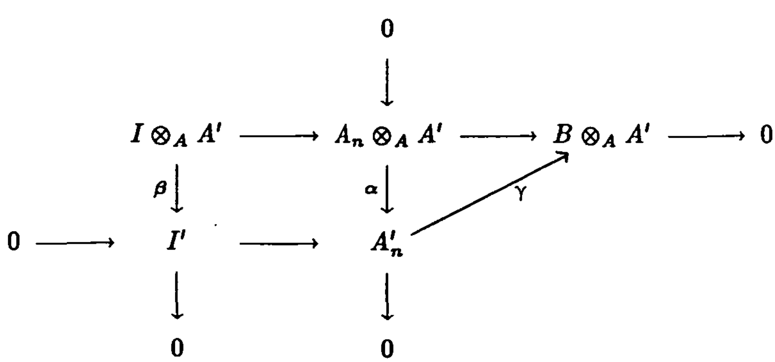
Lemma 1. *Let A be a ring, let I be an ideal in A_n, let $B = A_n/I$. Let A' be a ring containing A, with $A' \cap A_n = A$. Let I' be the ideal generated by I in $A'_n = A'[x_1, \ldots, x_n]$, let $B' = A'_n/I'$. Then*

(1) $B' \simeq B \otimes_A A'$,

(2) *if B is, as an A-module, finitely-generated and free with basis $\{f_1 + I, \ldots, f_r + I\}$ then B' is, as an A'-module, finitely-generated and free with basis $\{f_1 + I', \ldots, f_r + I'\}$, and, in this case,*

(3) *if g is in A_n, then $N_{A'}^{B'}(g + I') = N_A^B(g + I)$.*

Proof: (with our thanks to Jonathan Hillman). Tensor the exact sequence $0 \longrightarrow I \longrightarrow A_n \longrightarrow B \longrightarrow 0$ over A with A' to obtain the top row in the following commutative diagram:



https://doi.org/10.1017/S0004972700018244 Published online by Cambridge University Press

The map α is defined by $\alpha(f \otimes a') = a'f$ and linearity; it is the canonical identification of $A_n \otimes_A A'$ with A'_n. The map β is defined by $\beta(i \otimes a') = a'i$ and linearity; it is surjective since every element of I' is a sum of terms of the form $a'i$ with $a' \in A'$ and $i \in I$. The map γ is defined to make the triangle commute.

A routine diagram chase establishes that $0 \longrightarrow I' \longrightarrow A'_n \longrightarrow B \otimes_A A' \longrightarrow 0$ is exact, whence $B \otimes_A A' \simeq A'_n/I' = B'$. The rest of the lemma follows from basic facts about tensor products amd the definition of the norm. ∎

It follows from Lemma 1 that in proving the theorem we may assume $A = k$ is an algebraically closed field. We shall have need of the Hilbert Nullstellensatz, which we state as it appears in [5].

LEMMA 2. *If J is an ideal of $k_n = k[x_1, \ldots, x_n]$, if $f \in k_n$, and if $Z(J) \subseteq Z(f)$ then there is a non-negative integer m such that f^m is in J.*

4. PROOF OF THE THEOREM BY COMMUTATIVE ALGEBRA

We take as given the hypotheses of the theorem, with $A = k$.

LEMMA 3. *I has a reduced primary decomposition, $I = \bigcap_j Q_j$.*

PROOF: k_n is Noetherian. ∎

LEMMA 4. *For each j, $Z(Q_j)$ is a single point.*

PROOF: $Z(Q_j)$ is certainly a finite set, since $Z(I) = \bigcup_j Z(Q_j)$. Suppose $Z(Q_j) = S \cup T$, where S and T are disjoint and non-empty. Construct f, g in k_n such that f vanishes on S but not on T, and g vanishes on T but not on S (such f and g exist since S and T are finite sets and k is an infinite field). Then $Z(Q_j) \subseteq Z(fg)$, so, by the Nullstellensatz, $(fg)^m$ is in Q_j for some non-negative integer m. Since Q_j is primary, some power of f or g is in Q_j; but this is absurd, since f does not vanish on T and g does not vanish on S. ∎

LEMMA 5. *The Q_j are pairwise relatively prime.*

PROOF: For each j, let $Z(Q_j) = \{P_j\}$. If $r \neq s$ then $P_r \neq P_s$, since $I = \bigcap_j Q_j$ is a *reduced* primary decomposition. Assume P_r and P_s differ in coordinate ℓ, that is, $P_r = (\alpha_1, \ldots, \alpha_n)$, $P_s = (\beta_1, \ldots, \beta_n)$, with $\alpha_\ell \neq \beta_\ell$. Let $f(\underline{x}) = x_\ell - \alpha_\ell$, let $g(\underline{x}) = x_\ell - \beta_\ell$. Then $f(P_r) = 0$, so by the Nullstellensatz f^u is in Q_r for some non-negative integer u; similarly, g^v is in Q_s for some non-negative integer v. It follows that

$$0 \neq (\alpha_\ell - \beta_\ell)^{u+v-1} = (g - f)^{u+v-1} = f^u F + g^v G$$

for some F, G in k_n. Thus $Q_r + Q_s = k_n$. ∎

https://doi.org/10.1017/S0004972700018244 Published online by Cambridge University Press

Lemma 6. *$B \simeq \bigoplus_j k_n/Q_j$ (isomorphism as k-algebras).*

Proof: Chinese Remainder Theorem. ∎

Now let $B_j = k_n/Q_j$, and let m_j be the dimension of B_j as a k-vector space — this is the standard definition of the multiplicity of P as a zero of I.

Proof of the Theorem: Let $f \in k_n$. Then for each j, $(f + Q_j)B_j \subseteq B_j$, so $N_k^B\overline{f} = \prod_j N_k^{B_j}(f + Q_j)$. Let T_j be the restriction to B_j of the linear operator, "multiplication by $\overline{f}$", and let λ be an eigenvalue of T_j with corresponding eignevector $b \neq 0$. Thus $(f + Q_j)b = \lambda b$. Let $b = v + Q_j$ for some $v \in k_n$; then $(f - \lambda)v \in Q_j$. Now $b \neq 0$ implies $v \notin Q_j$. Since Q_j is primary, there is a positive integer m such that $(f - \lambda)^m \in Q_j$. Thus $(f(P_j) - \lambda)^m = 0$, so $\lambda = f(P_j)$. Hence $N_k^{B_j}(f + Q_j) = f(P_j)^{m_j}$, whence $N_k^B\overline{f} = \prod_j f(P_j)^{m_j}$. ∎

5. Proof of the theorem by linear algebra

We present a second proof which does not involve primary ideals or the Chinese Remainder Theorem (at least, not overtly). We let $Z(I) = \{P_1, \ldots, P_\ell\}$.

Lemma 7. *Given f, g in k_n with $fg \in I$, if $Z(f) \cap Z(I) = \phi$, then $g \in I$.*

Proof: Let $h = \prod_{j=1}^{\ell} (f - f(P_j))$. Then $Z(I) \subseteq Z(h)$ so, by the Nullstellensatz, h^m is in I for some non-negative integer m. Thus $h^m g$ is in I. Now $h^m = fr + c$ for some $r \in k_n$ and some non-zero c in k — in fact $c = (-1)^{\ell m}\left[\prod_j f(P_j)\right]^m$. So from $h^m g$ in I we deduce $frg + cg$ in I, whence cg is in I, whence g is in I. ∎

Lemma 8. *Let T_f be the linear operator on B given by multiplication by $\overline{f}$. Then the eignevalues of T_f are precisely the quantities $f(P_j)$, $j = 1, 2, \ldots, \ell$.*

Proof: Assume $T_f b = \lambda b$ for some non-zero b in B and some λ in k. Choose g in k_n such that $b = g + I$; note that $b \neq 0$ implies g is not in I. Then $(f - \lambda)g$ is in I. By Lemma 7, $Z(f - \lambda) \cap Z(I) \neq \emptyset$; hence, $\lambda = f(P_j)$ for some j.

Conversely, for each j, choose u_j in k_n such that $u_j(P_r) = \delta_{jr}$. Such polynomials are easily constructed explicitly, and we omit the details. Let $v_j = (f - f(P_j))u_j$. Then $Z(I) \subseteq Z(v_j)$, so, by the Nullstellensatz, $v_j^m = (f - f(P_j))^m u_j^m$ is in I for some positive integer m. On the other hand, u_j^m is not in I, since $u_j^m(P_j) \neq 0$. So there is an integer r, $0 \leqslant r < m$, such that $(f - f(P_j))^r u_j^m$ is not in I but $(f - f(P_j))^{r+1} u_j^m$ is. Let $w_j = (f - f(P_j))^r u_j^m$; then $\overline{w}_j$ is an eigenvector for T_f with corresponding eigenvalue $f(P_j)$. For, $T_f\overline{w}_j = fw_j + I = (f - f(P_j))w_j + f(P_j)w_j + I = f(P_j)w_j + I = f(P_j)\overline{w}_j$. ∎

It follows from Lemma 8 that for every f in k_n there exist positive integers $m_1, \ldots, m_\ell$ such that $N_k^B \overline{f} = \prod f(P_j)^{m_j}$. To conclude the proof of the theorem it remains only to show that the m_j can be chosen independently of f.

PROOF OF THE THEOREM: Choose h in k_n such that $r \neq s$ implies $h(P_r) \neq h(P_s)$. Let $B = B_1 \oplus \ldots \oplus B_\ell$, where B_j is the eigenspace of T_h corresponding to the eigenvalue $h(P_j)$, $j = 1, \ldots, \ell$. Let $m_j = \dim_k B_j$. By Lemma 8, each m_j is positive. It is clear that $N_k^B \overline{h} = \prod h(P_j)^{m_j}$.

Now for $j = 1, \ldots, \ell$ let u_j be as in the proof of Lemma 8. By the argument of that lemma, $(h - h(P_j))^m u_j^m$ is in I for some integer m. Equivalently, $(T_h - h(P_j))^m \overline{u}_j^m = 0$, so $\overline{u}_j^m$ is a non-zero element of B_j.

Now let f be an arbitrary element of k_n. Since T_h and T_f commute, B_j is an eigenspace for T_f. Let λ be the corresponding eigenvalue. Then there is an integer r such that $(T_f - \lambda)^r \overline{u}_j^m = 0$, that is $(f - \lambda)^r u_j^m$ is in I. Evaluating at P_j, and recalling that $u_j(P_j) \neq 0$, we see $(f(P_j) - \lambda)^r = 0$, so $\lambda = f(P_j)$. The theorem now follows. $\square$

We note that this proof presents an alternative method of viewing the multiplicity of a zero P_j of the ideal I, namely, as the dimension of the generalised eigenspace B_j corresponding to the eigenvalue $h(P_j)$ of an operator T_h, where h is such that $r \neq s$ implies $h(P_r) \neq h(P_s)$.

6. RESULTANTS

Let A be a commutative ring with unity. Let f and g be polynomials with coefficients in A. The resultant of f and g, written $R(f, g)$, is defined to be the determinant of the Sylvester matrix; this is the matrix

$$\begin{bmatrix} a_n & a_{n-1} & & \cdots & a_0 & & \\ & a_n & & \cdots & & a_0 & 0 \\ 0 & & \ddots & & & & \ddots \\ & & & a_n & \cdots & & a_0 \\ b_m & b_{m-1} & & \cdots & b_0 & & \\ & b_m & & \cdots & & b_0 & 0 \\ 0 & & \ddots & & & & \ddots \\ & & & b_m & & & b_0 \end{bmatrix}$$

where $f(x) = \sum_{j=0}^{n} a_j x^j$ and $g(X) = \sum_{j=0}^{m} b_j x^j$, $a_n \neq 0$, $b_m \neq 0$ (in the matrix the coefficients of f fill m rows, and the coefficients of g fill n rows).

If A is an integral domain then there are well-known expressions for $R(f, g)$ in terms of the zeros of f and/or g, for example

$$R(f, g) = a_n^m \prod g(\alpha),$$

where α runs through the zeros of f in a splitting field containing A, with multiplicities. Comparing this with the theorem yields

COROLLARY 1. *Let A be an integral domain. Let f in A_1 be monic. Let $B = A_1/(f)$. Then for all g in A_1 we have*

$$R(f, g) = N_A^B \bar{g}. \tag{2}$$

Both sides of (2) are defined in terms of the coefficients of f and g alone, from which it follows that (2) holds under the weaker hypothesis that A be a commutative ring with unity. This attractive result has been discovered independently several times. Professor Schinzel informs me that a formula equivalent to (2) appears in a work of Čebotarev [**2**] to which I have not had access; since then it has appeared in [**6, 4, 9, 1, 10**], and, we regret, [**7**].

We would like to generalise Čebotarev's result to multivariate polynomial rings. There are difficulties with resultants of systems of multivariate polynomials that do not arise in the one-variable case, but our theorem suggests that here, too, norms and resultants are very closely related — see also the expression for the resultant given by Netto [**8**]. We hope in a later paper to expand on the relation between the norm as presented here and the resultant of a system of multivariate polynomials.

REFERENCES

[1] S. Barnett, 'Greatest common divisor of two polynomials', *Linear Algebra Appl.* **3** (1970), 7–9.

[2] N.G. Čebotarev, *Teorija Galua* (Mathematika w Monografijach, Serija Obsorow I, Moskwa, Leningrad, 1936).

[3] W. Gröbner, *Moderne algebraische Geometrie* (Springer, Vienna and Innsbruck, 1949).

[4] R.E. Kalman, 'Mathematical description of linear dynamical systems', *SIAM J. Control* **1** (1963), 152–192.

[5] S. Lang, *Algebra* (Addison Wesley, Reading, Mass., 1965).

[6] N.H. McCoy, 'Divisors of zero in matric rings', *Bull.Amer.Math.Soc.* **47** (1941), 166–172.

[7] G. Myerson, 'On resultants', *Proc. Amer. Math. Soc.* **89** (1983), 419–420.

[8] E. Netto, *Vorlesungen über Algebra, vol II* (Leipzig, 1900).

[9] H. Schmidt, 'Bemerkung zur elementaren Algebra : I. Restklassenring und Resultante', *Bayer. Akad. Wiss. Math. - Natur. Kl. Sitzungsber. 1966* **II** (1967), 167–172.

[10] W.G. Vogt and N.K. Bose, 'A method to determine whether two polynomials are relatively prime', *IEEE Trans. Automat. Control AC–15* (1970), 379–380.

Department of Mathematics
Macquarie University
New South Wales 2109
Australia